(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005年10月20日 (20.10.2005)

PCT

(10) 国際公開番号
WO 2005/098796 A1

(51) 国際特許分類[7]: G09C 1/00

(21) 国際出願番号: PCT/JP2005/005287

(22) 国際出願日: 2005年3月23日 (23.03.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-102399 2004年3月31日 (31.03.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 寺西 勇 (TERANISI, Isamu) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 丸山 隆夫 (MARUYAMA, Takao); 〒1700013 東京都豊島区東池袋2-38-23 SAMビル3階 丸山特許事務所 Tokyo (JP).

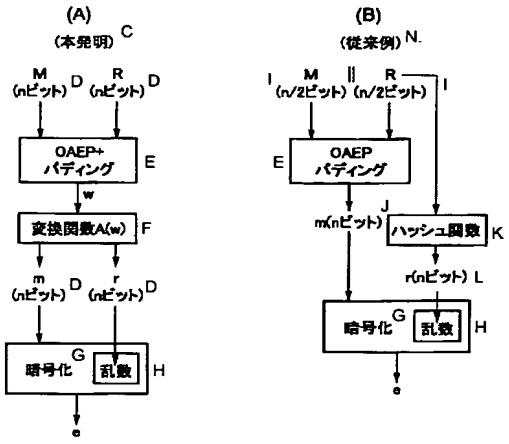
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,

[続葉有]

(54) Title: PADDING APPLICATION METHOD GUARANTEEING SAFETY OF ENCRYPTION METHOD

(54) 発明の名称: 暗号方式の安全性を保証するパディング適用方法



C... THE PRESENT INVENTION
D... n BITS
E... OAEP + PADDING
F... CONVERSION FUNCTION A(w)
G... ENCRYPTION
H... RANDOM NUMBER
N... CONVENTIONAL EXAMPLE
I... n/2 BITS
J... m(n BITS)
K... HASH FUNCTION
L... r(n BITS)

(57) Abstract: There is provided an encryption/decryption device achieving a safe encryption communication by performing an appropriate padding to a method such as an NTRU encryption method. An n-bit plain text M is received and subjected to OAEP+ padding. The result is subjected to a conversion A satisfying the following condition so as to obtain two bit strings m and r. The conversion A is mapping for correlating elements $L_m \times L_r$ to a bit string of k bits or below. When L_m represents a range of m and L_r represents a range of r, the next condition should be satisfied: the mapping is an injection; A and its inverse mapping can be calculated by polynomial time; when the encryption function is E(m, r), the mapping $E:A(X) \rightarrow L_e$ is a uni-directional function. The X represents a range of (m, r) and L_e represents a space of the entire encrypted text. After division into m and r, $e = E^r(m)$ is calculated and encrypted and the e is transmitted to a receiver of the encrypted text.

(57) 要約: NTRU暗号方式のような方式に対して適切なパディングを施すことで安全な暗号通信を達成する暗号化/復号化装置を提供する。 nビットの平文Mを受け取りOAEP+パディングを行い、その結果を次の条件を満たす変換Aを用いて2つのビット列mとrを得る。変換Aは、kビット以下のビット列に$L_m \times L_r$の元を対応させる写像であり、L_mはmの取りうる範囲、L_rはrの取りうる範囲であるとすると、次の条件：単射であること、Aおよびその逆写像は多項式時間で計算できること、暗号化関数をE(m,r)とした時に写像$E : A(X) \rightarrow L_e$は一方向性関数であること、を満たす必要がある。ただしXは(m,r)の取りうる範囲を表し、L_eは暗号文全体の空間を表す。mおよびrに分割されると、$e = E^r(m)$を計算して暗号化し、eを暗号文受信者に送信する。

WO 2005/098796 A1

IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。